User Perceived Privacy

Mental Models of Users' Perception of App Usage

Sørensen, Lene Tolstrup

Published in:
Nordic and Baltic Journal of Information and Communications Technologies

DOI (link to publication from Publisher):
10.13052/nbjict1902-097X.2018.001

Publication date:
2018

Document Version
Publisher's PDF, also known as Version of record

User Perceived Privacy

Mental Models of Users' Perception of App Usage

Lene Sørensen

Center for Communication, Media and Information Technologies,
Aalborg University, Denmark
E-mail: ls@cmi.aau.dk

Received 08 October 2018;
Accepted 29 October 2018

Abstract

Information privacy is jeopardized almost every time a person uses digital services or applications. The European General Data Protection Regulation, GDPR, recognizes that to empower the users and put focus on privacy, in the future all software (as well as applications) must provide transparency and consent so that the users are protected and are able to manage their privacy in contrast of today. This paper researches the perception of privacy in use of three selected applications; Endomondo, MobilePay and Roskilde Festival apps. In an empirical study, participants have been instructed to draw mental models of different use situations of these applications and to discuss where there needs to be a privacy notification or other to inform the user about the sharing of private data – as announced by the GDPR framework. The work constitutes the first step in a process of understanding the design challenge of the GDPR and for suggesting privacy related design for the interface design with a focus on the user experience.

Keywords: Privacy, mental models, GDPR, privacy notices, usable privacy.

Journal of NBICT, Vol. 1, 1–20.
doi: 10.13052/nbjict1902-097X.2018.001

1 Introduction

The Statistica (2017) forecasts that by 2020, mobile applications will generate around 189 billion US dollars via app stores and in-app advertising. According to (Vallina-Rodriguez and Sundaresan, 2017) 7 out of 10 of applications include third party access where private information is being shared, sold and transferred to services often outside the knowledge of the users. Information about who uses the app, GPS coordinates, preferences in music, contacts etc. can be part of the data being shared or sold (ibid). Lipert (2015) says ".. every new device, app, and social network is now assumed to come with hidden privacy risks." The privacy of users can be said to be challenged and without the possibility of rejecting this if the users wants to use applications.

In Europe, the so-called GDPR (General Data Protection Regulation) Framework (EC, 2016) has come into force in 2018. The main purpose of this GDPR framework is to secure personal data of EU users through data transparency, management and governance (ibid). Fundamentally, every user in Europe must be given possibilities of choice and consent in opposition to todays' take-it or leave it policies in many digital services. This means that the user to some extent needs to be able to interact with the services, see data which are being used for services and to select which data should be used and which not or even deleted completely. Transparency, consent and privacy by design (Centre for Information Policy Leadership, 2017) are the foundations for the GDPR to change the empowerment towards the users.

For years users have been presented with different forms of privacy notifications, consent forms and in some cases privacy profiles however these often fail to inform the user about what really happens to the private data and has failed in providing informed choices for the users (Schaub et al., 2015). Within the field of usable privacy different initiatives have been presented such as for example the Privacy Bird (Cranor et al., 2005) however with no broad acceptability and use resulting. Also, many privacy management tools have been developed as for example GOTCHYA (Lindow-Zechmeister, 2017) but again, these tools are on a voluntary basis and do not have a broad acceptability and usage. Studies (as Rainie and Duggan, 2015) show that users generally feel lost when thinking about privacy and that there is a need to support the users' understanding, control and management through clever interface design.

The purpose of this paper is to propose privacy statements/notifications and privacy interface design in relation to three selected applications.

The applications have been selected from the perspective of broad usage of different specific groups and a track record for their usage. The Endomondo fitness application is used worldwide to track fitness activities of the user and provide feedback for further motivation (endomondo.com). The MobilePay application is the payment application which is most popular in Denmark, for payment between peers as well as in shops (mobilepay.dk). The Roskilde Event Application has around 60.000 users every summer when the Roskilde Festival takes place for 10–12 days in July (IBM, 2015). The Roskilde Event app provides information on the festival music program, where to go for food and recommendations on music from the users' Spotify lists etc. (roskildefestival.dk). The MobilePay app is the 4th most downloaded app in Denmark 2017 (Olsen, 2017). The Roskilde Festival app is one of the apps recommended when 130.000 participants participate in one of Europe's biggest festivals and in that way, create a micro-environment for the 10 days it lasts (IBM, 2015).

To propose privacy statement/notifications and other interface design elements related to privacy, this paper takes a first step in understanding how users' mental models about the data flow when it comes to the usage of the three applications. The mental models (Nielsen, 2010) are seen as one way of understanding how users think about the applications and how they work and as an entrance to talk about privacy. After the mental models, it is discussed with the users where they see their privacy jeopardized and what do to about it.

This approach follows the idea from Kang et al. (2015) where they investigated mental models of Internet as a basis for privacy and security discussions. Understanding of mental models are furthermore recognized to be a starting point of user experience design (Nielsen, 2010). This work shall be seen as a first step in understanding how users think about privacy and their application usage.

The paper is organized as follows: The Section 2, describes existing privacy definitions, representations and initiatives as a background for the paper. Furthermore, the GDPR Framework is described and discussed in relation to the existing privacy initiatives. In Section 3, the methodology of the paper is described focusing on the empirically made mental models and the background of the design process as used in the paper. In Section 4, the empirical work is presented with respect to the mental models and the discussions on privacy made with a group of users. Section 5 discusses the results of the paper and compares these with the existing privacy services and the requirements in the GDPR. Finally, conclusions are presented in Section 6.

2 Privacy

In the survey made by Rainie and Duggan (2015) it is said Americans are willing to exchange personal data for benefits (such as app usage) but also that they are unhappy about the situation where the data collected by a company is used for something else afterwards (for example sold to other parties). In this paper (ibid), it is concluded that the difference between disclosure or personal information and privacy is dependent on the situation. Such a conclusion blurs how privacy can be defined and perceived.

2.1 Information Privacy

In the literature, privacy is often denominated by information privacy relating to the privacy of personal information. Clarke (2000) refers to "the right or ability of individuals to exercise control over the collection, use and disclosure to others of their personal information." Lately, Ziegeldorf et al. (2014) have defined information privacy based on the IoT (Internet of Things) architecture:

> *"Privacy in the Internet of Things is the threefold guarantee to the subject for i) awareness of privacy risks imposed by smart things and services surrounding the data subject; ii) individual control over the collection and processing of personal information by the surrounding smart things; and iii) awareness and control of subsequent use and dissemination of person al information by those entities to any entity outside the subject's personal control space."*

This definition is linked to the IoT architecture and presents privacy with this IoT architecture in mind. However, the above-mentioned definitions focus on the users to be aware and have control in relation to the surrounding smart things or services.

Cavoukian and Chibba (2018) describe the information privacy as "the right to exercise one's right to decide who to choose to share the personal details of one's life with."

In this paper (ibid) it is made clear that information security not equals privacy but that information privacy incorporates a broader set of protections than security alone. The paper (ibid) furthermore agitates that all application developments should be based on the principles of Privacy by Design which are integrated into the GDPR framework (as will be seen later).

In the already mentioned paper by Rainie and Duggan (2015) focus groups were run amongst groups of Americans. In these focus groups, the

element of "bargaining" was introduced as a possibility to discuss the trade-off between the service provider and what the participants would want from the service. This survey showed that initial bargains would be fine with a direct bargaining between the user and the service provider. However, bargains between the user and the companies that collect data would be annoying and unwanted. This scenario tells specifically that users disclose private information if there is a wanted achievement but they do not have an interest in the more economical bargain with third parties which not directly have a win for the user. Furthermore, there is a worry that the information that these companies collect not are protected well enough. Such a study shows that it is difficult to define precisely the concept of privacy since it changes with situations.

2.2 GDPR: Transparency and User-Centricity

For years, the European Commission has worked to develop the General Data Protection Regulation, GDPR (EC, 2016). The purpose of this is to protect "natural persons" with regard to processing of personal data and the free movement of this data. As such the GDPR can be seen as a result of the focus the EU has had on the usage of digital services across Europe and the enormous collection and sharing of personal data across borders and public/private sectors. The GDPR is an attempt to secure the privacy of persons in Europe and the users' right to protect and manage their personal data (EC, 2016).

The General Data Protection Regulation consists in total of 11 Chapters and 91 Articles (EC, 2016). In the Articles 17 and 18 specifically focus on providing data subjects (private users) more control over personal data that is processed automatically (ibid). Personal data is defined by:

"Personal data" means any information relating to an identified or identifiable person (data subject), and identifiable natural person is one who can be identified directly or indirectly, in particular by reference to an identifier such as name, an identification number, location data, online identifier or to one or more factors specific to the physical, psychological, generic, mental, economic, cultural or social identify of that person" (EU, 2016a).

This means that "Under the GDPR any cookie or other identifier uniquely attributed to a device and therefore capable of identifying an individual or treating them as unique even without identifying them is personal data" (Beaumont, 2016).

Center for Information and Policy Leadership (2017) explains as a central element in the GDPR is transparency and consent to secure fair processing

principles and privacy notices with truly and meaningful information to the users. In that way, the GDPR centers around the user and have a very user-centric approach (ibid). It is said that transparency should be "... context-specific, flexible, dynamic and adaptable to constantly evolving and changing uses to provide clear and understandable information to individuals and enable genuine choice..." (ibid).

The perspective of the user-centricity is furthered in Article 25 (EC, 2016a), where it is detailed that the principles of "privacy by design" and "privacy by default" must be evoked.

2.3 Digital Initiatives on Privacy Management

As already mentioned, there exists a number of privacy initiatives already implemented or being researched.

Generally Implemented Privacy Initiatives

The Terms of Service, ToS, presents the conditions for use of a particular service that the service provider and the user basically agree on before the service can be used. Often the ToS is a rather lengthy document that can take up to 15–20 minutes to read (Lamm, 2016). Many surveys and research show that users generally not read the ToS (Lamm, 2016; Berreby, 2017; Tos, DR, 2012). Lamm (2016) constructed a fictions social network with Terms of Service including a section which said that the user would assign their first-born child to the company. Out of 527 participants only 9 participants found this paragraph and declined to agree to the ToS, other participants spend between 1 and 5 minutes on the Terms of Service (which was estimated to be read within 15–17 minutes) (ibid). A similar study is made by Berreby (2017). It is concluded that the ToS is a lengthy document often with legal language, that many users simply not read. The website Terms of Service. Didn't Read (ToS, DR, 2012) is a service which make a shortened version about any ToS that the user can use in an app either on the laptop or on the mobile.

The so-called privacy setting is a service that service providers can provide to users to draw attention to privacy and to provide the users with some control of their privacy and how public their data should be shown to others. It is often seen with social media services (for example Facebook Basic Privacy Settings) and browser services such as Google Privacy Control. In a study made by Rainie and Duggan (2016) it was shown that particular teens (60% of these) are using the privacy settings on social media to keep their profile private and they have a high confidence in that they understand the management

of their privacy. The same study (ibid) shows that teens are not worried about the sharing of data for third parties (only 9% expressed that they were worried about this). Facebook has often been mentioned as a service where the privacy settings are easy to follow and where they actually matter. Same study (ibid) say that teenagers think that it is easy to use the privacy settings using Facebook.

The cookies consent law was enforced by the European Union in 2011 (Beaumont, 2016). It is a part of the EU's focus on privacy and data protection where the cookie consent shall inform the user that the service they are about to use explain to the users that information about them not is collected unnecessarily (ibid). The cookie consent is often made as a popup on the landing page of a website. Titcomb (2016) express that the cookie consents presented for users of Internet websites often not say anything precisely about what happens to users' data and they are considered to be irritating and annoying. It is currently discussed that the user should have privacy settings set in the internet browser settings to get rid of the cookie consents (ibid).

Selected Privacy Initiatives and Research

There are many initiatives originating from individual research groups and organizations which also bring focus on privacy and how to control and mange. One of these initiatives is the so-called Privacy Bird which finds websites that comply with the privacy settings of the user (Cranor et al., 2005). The Privacy Bird reads privacy policies written in the format of the World Wide Web consortium (P3P – ibid) and can be installed free of charge to indicate to the user with a green bird if the website is compliant with the privacy settings of the user and a red bird if not. When the software is installed a bird-icon appear in the top title of the website as an add on icon (ibid).

Another initiative is the so-called "Nutrition Label" (Kelley et al., 2009). In Kelley et al. (2009) a privacy nutrition label is suggested with a table like information on the context for the information, short labels for row and column headers, information on what is not collected, a scale from light to dark used to display how severe privacy practices are etc.

In the line with the Privacy Bird, there exists multiple privacy control and management tools developed as apps to monitor or visualize data streams, companies interested in the users' private data etc. (see for example Khajuria and Sørensen, 2015). However, these tools are only if users have a special interest in privacy and only to find specific areas of privacy.

Furthermore, work is ongoing to develop a set of icons for use in standardized information policies (Pettersson, 2012). This work has developed

around informed consent as prescribed by EU regulations and laws. Others have attempted to include icons to be integrated in the top bar of the browser (for example Cranor et al., 2005). The European Union's work on Privacy and Data Protection has also included privacy icons (EC, 2016). The work is still underway but the hope is to make sure that a set of privacy icons can be used in Interface Design in the future.

3 Methodology

Based on the principles from "privacy by design" by Cavoukian and Chibba (2018), this paper has taken the methodological angle to be user-centric and start with an understanding of how users think. Mental models have been used as a starting point to discuss privacy with a group of user/participants. A mental model is a well-recognized way to start a design process (Nielsen, 2010). In short, a mental model is a model of the users' belief of how a specific service works or should work (Nielsen, 2010). It can be a description or a drawing of how a flow of data or how a specific internet service works (Kang et al., 2015). The mental models have been used to identify where a group of user would think that their privacy could be violated as a means to discuss what type of design element there would be needed to comply with the GDPR framework.

The above-mentioned approach to discuss design with potential users is based on Shneiderman and Hochheiser (2001) The design process Shneidermand and Hochheiser (2001). The design process, Shneidermann and Hochheiser (2001) describe, starts with understanding the gap between with what users know and what they need to know – that users must start with a low complexity to be able to understand a more comprehensive and complex level of the interface design. This paper therefore follows the idea from Kang et al. (2015) where they start with discussing mental models of users as a basis for discussing privacy and security.

This paper, however, has a focus on three selected applications, and to secure that the users would be able to draw mental models of their thinking about how these applications work, task-scenarios (NN Group, 2014) were set up. The task-scenario approach secures that the users quickly can focus on one or two tasks that they would be able to do with the applications compared with a multiplicity of tasks it would be difficult and time consuming to look at all together.

3.1 In Practise

The work centers on a workshop carried out with 15 participants (12 male and 3 female) all students at the ICTE Master Education at AAU, Denmark, October, 2017. The workshop was carried out as a part of course on "Cyber Security and Trust" which is why the students already had heard about privacy as a concept and the GDPR. The participants also had prior knowledge about IT and various networks.

It was decided to work with applications that was a high likelihood that the participants knew beforehand so they not should spend extra time in trying to understand the application and its services. Applications were chosen for this research as examples of services which will be in focus in the GDPR and where there today not exists many privacy notifications or other privacy enhancing elements. The three applications in focus were: Endomondo fitness application, MobilePay application and the Roskilde Festival application.

The Endomondo application (endomondo.com) supports users to be and stay active in all sorts of sports. The application tracks, logs and analyzes fitness, provides audio support and can synchronize with other users of the app. The MobilePay application (mobilepay.dk) is a payment app which works between peers as well as in many shops. The application pays through the phone number of the shop or other person and it keeps the user's credit card information so that the users will not have to write that every time there is a payment. The Roskilde Festival App (Roskilde-festival.dk) includes information on the festival's music and good places to eat, it can also link to Spotify to provide recommendations on which bands to listen to at the festival.

The participants were divided into three groups each group working with one specific application. The groups were equally large with 5 persons in each. The division into groups was based on the participants' prior knowledge of the applications in focus and their willingness to work with this. Each participant was then instructed to draw how they envision the data flow is when using the application in specific use situations (tasks). It was up to the groups themselves to decide how this representation should be in mental models of how the application works.

In order to make sure that the participants could understand different situations of app usage, a task-scenario (NN Group, 2014) was used to ensure that the participants had a common understanding of the application and how it worked in a variety of use situations.

For participants with a focus of the Endomondo application the task scenarios were:

1. Imagine you are preparing for a run in the surroundings of the South Harbor in Copenhagen. You want to make sure that you have an idea of how far you have run and where you have run for statistics. Make a drawing of the data which is created when you run with the Endomondo application.
2. You think you have run fast and would like to share and compare with other runners on a similar (if not the same) route. So now you share your data with others by use of the application. Make a drawing of the data and where it goes to be shared and compared with others.

For participants with a focus of the MobilePay application, the task scenarios were:

1. Imagine you are out with your friends and that you want to buy some food at a food stand. The food stand allows you to use your MobilePay application and you therefore ask for the food and pay. Make a drawing of the data which is created when you pay for the food with the MobilePay application.
2. On your way home, you want to have a coffee from seven/eleven. This shop allows you to pay directly with your app via their register where you just keep your device close to their register and the payment happens. Make a drawing of the data and what takes place when you pay in this way.

For participants with a focus on the Roskilde festival the task scenarios were:

1. You have arrived at the Roskilde Festival and now you want to have an overview of where you can eat and how far you are from some of the best eating places. Make a drawing of how the application provides you with this information by thinking about the data flow and where it goes.
2. You do not know all the bands playing and therefore wants to have some recommendations on the music selection. You use the Roskilde Festival app to give you these recommendations based on your use of Spotify. Make a drawing of the data which flows in this situation.

Each group was provided with paper and the possibility to ask the author about uncertainties in the tasks.

After the mental models were drawn, the participants were encouraged to discuss whether they would be able to foresee any privacy challenges when looking at their mental model. Additionally, the groups were instructed to discuss how they would envision that this could be solved in the interface design. The groups were only instructed to think about the design of the privacy interface design as a conceptual element and not as a tangible new drawing.

The groups, finally, presented the results for each other and the drawings, and a summary of the results presented was written down by the author.

For the analysis, the mental models have been used to discuss how the participants' perception of privacy have been and to discuss the results that came across the workshop.

4 Users' Mental Models

Mental models were produced based on discussions and drawings made from participants of a workshop.

4.1 Settings

The three groups worked in a class room and in an adjacent room. They were given 30–60 minutes to do the mental model and to identify the privacy elements.

Since the participants were asked to make a drawing as their understanding of the service would be these drawings represent the mental models. The groups had some discussions internally about how the mental model should be defined, if it was a data flow diagram or a storyboard. For that reason, the author took rounds with the groups to take these discussions and to define the mental model as a high-level diagram describing the entities, the data and other important elements that they would foresee.

Each group discussed about a common mental model and did one drawing. After the drawings, the groups discussed the potential for violation of the GDPR rules on transparency and control with respect to the mental models. After that they discussed how to comply with that in an interface design.

4.2 Results

Endomondo

In Figures 1 and 2, the mental models of the group working with the Endomondo tasks are presented. The Figure 1 are linked to the first task where the group was asked to discuss what happened when they used the Endomondo app for run. The Figure 2 presents the mental model where the data from the run would be saved with others (friends).

In these diagrams (Figures 1 and 2), the participants chose to focus on the mobile device to show the selection of different services and let that be the starting point of the communication with other entities/devices. In the Figure 1, the mental model show that the group perceive that there is a kind of exchange of information between the device and a satellite to map the route and later a database to save this for future use. The group indicate that the applications measures data such as time, GPS coordinates, heart beat and calories. The group did not see any particular privacy problems with this approach and therefore did not suggest any privacy initiatives to be implemented.

In the Figure 2, the Figure 1 is extended with a link via Facebook where peers are contacted through Facebook to share the data and to be able to compete via the application. The group discussed that the usage of this data and data from Facebook would need a consent to put focus and be more transparent for the user.

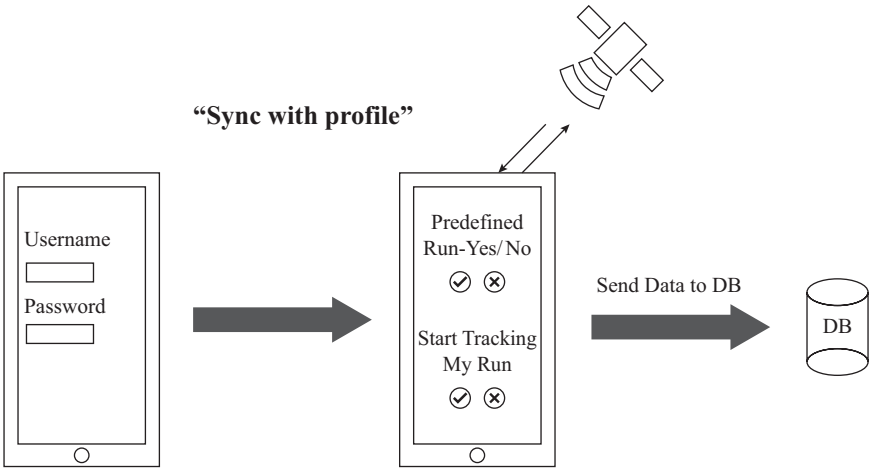

Figure 1 Mental model of the use of Endomondo app during a run.

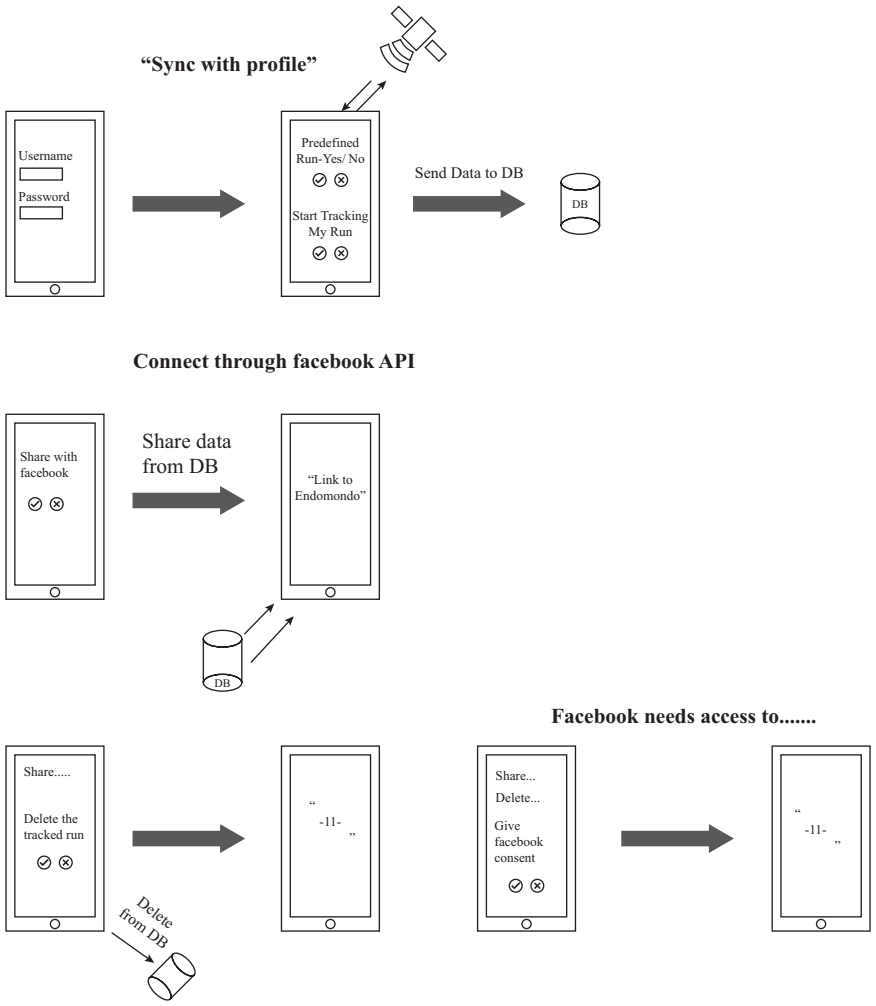

Figure 2 Mental model where the Endomondo Application is used for a run and data shared with peers. This mental model includes the first mental model (in Figure 1) first since that part is happening first.

MobilePay

The MobilePay application is in use many times each day for a lot of users. The group did not have any difficulties in agreeing on what happened in the two tasks. Figure 3, presents the mental model, the group made discussing what happened when payment happened between peers.

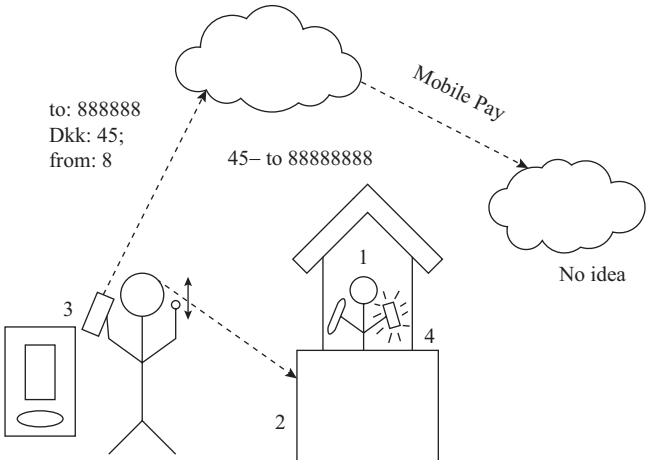

Figure 3 Mental model of paying with the MobilePay application between peers.

In Figure 3, the first task is described where a person pays to another person. The group describes the data that the user delivers to the payment situation (phone number on the receiver, the amount and information on who sent the money). This data goes to a service in the cloud (they explained it was MobilePay) and then there would be a communication between another cloud service (the bank) before the payment go to the receiver. They agreed that this process was without any privacy problems and the data and communications are necessary for the service.

Figure 4, presents the situation where payment takes place between a more established shop (fx. Supermarket) with the cashier and the users' mobile phone.

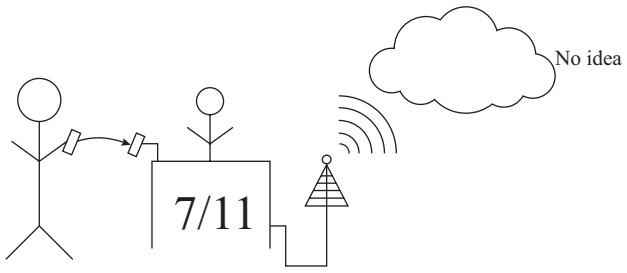

Figure 4 The mental model of how the payment is done in a shop using the MobilePay application and a cashier.

In the Figure 4, the second task was discussed. Here, the communication took place with almost the same flow and data as the first example (the group agreed that the example was to buy something in a seven-eleven store). After this, the group found that it could be a problem that the service provider could see the user's phone number after the transaction. They considered that this in some situations could be an unwanted exchange and that is not would be relevant in many situations that the service provider would have that data afterwards. The group discussed that the application could manage this by a notification to the user asking about this information should be visible or not.

Roskilde Festival

The Roskilde Festival application is used for many different things, both for information on the festival music and services but also on where to find the nearest toilet and recommendations on music based on the user preferences. The Figure 5 presents the mental model that the group agreed on when the task was looking for a good place to eat at the festival.

The group considered that the festival app on the mobile would communicate the location to the Festival Services and that the request would return with information on location and the food place. Discussions were about whether there also was a communication between the Festival service and another service (they could not agree on what that would be and therefore there are nothing in the mental model). They discussed that the location could be a private data but since the user requested the information, they thought there wouldn't be a need for a notification.

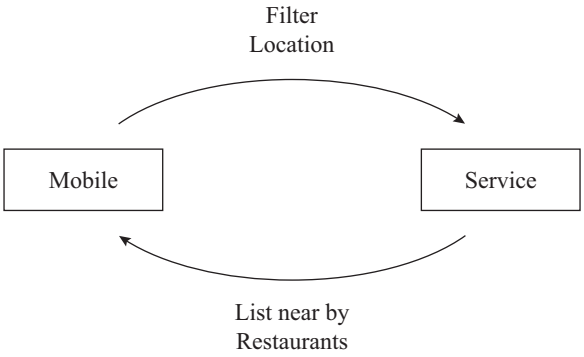

Figure 5 Mental model for looking for a good place to eat at the festival.

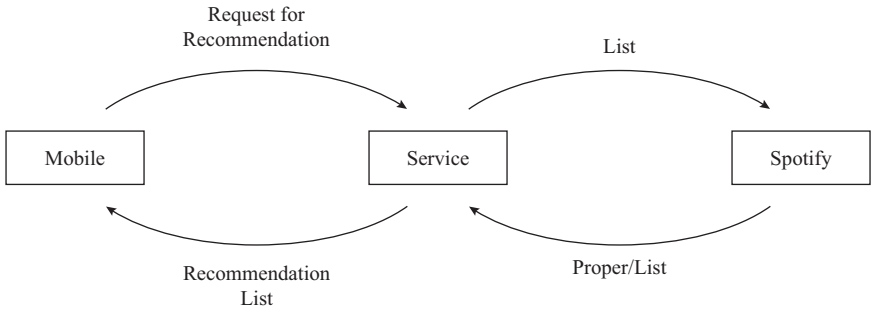

Figure 6 Mental model of receiving information on playlists for Spotify as a basis for recommendations to music at the festival.

In the Figure 6, the mental model of the second task where the group should discuss what happened when they would get a recommendation in the festival app based on their preferences of music from Spotify.

The mental model in Figure 6, describes again the mobile phone and a first communication to and from the festival services and then communication between these and the Spotify service. The group discussed that the communication between Spotify and the Festival Services should be accepted with a consent or notification to let the user know about this link and the exchange of personal preferences.

5 Discussion

Generally, the participants did not see the privacy to be a significant challenge. They accepted that there could be found some privacy challenges in the direct interaction between peers or through use of other services, but they did not question or think that there is a challenge in sharing private data such as heart beat and GPS locations. Furthermore, the participants did not discuss the potential for third parties interfering with the services in some way and therefore missed a significant discussion on the transparency and privacy discussed in the GDPR. This could fall back to the method used for the developments of the mental models

Reflecting on the methodology, the task-scenario perhaps were too restricted for the participants to use. In Kang et al. (2015) they have investigated mental models for how the Internet works and working with a much more open task for the participants themselves to choose what the mental model should be around. This could also be done in future work on this study,

so that the participants select the activities they would like to do based on their experiences with understanding and using the applications already. In that way, they could be more motivated to discuss the privacy perspectives in activities they would do instead of a thought, pre-selected activity.

Another perspective is the mental model which was introduced for the participants. The mental model as a concept was unknown to most of the participants and therefore, the participants were a bit confused in the beginning and spent some time in discussing (also with the authors) what that means. Again, a freer way of describing what and how they foresee the services and what happens with respect to data, and communication channels did not have to be framed as a mental model. The participants would therefore be allowed to use more creativity and perhaps create representations closer to their mental model than the representations seen in the Figures 1–6. It shall be noted that most of the students had a course in Interaction Design, and that it therefore was assumed that the students knew about the concept of a mental model.

The participants had no difficulties to discuss and understand the privacy aspects of the GDPR. These participants were taking a class on security and privacy, they therefore probably had an advantage compared to others. For future work, there is a need to discuss privacy aspects with participants to be certain that they understand the concept.

The results of the exercise described in Section 4, was that the participants mainly pointed to notifications or consent forms to handle the privacy aspects they found. For future work, it could be relevant to set up sessions focusing on the specific interface designs (conceptually) and for testing these to get a deeper insight to how these privacy aspects can be handled without jeopardizing the user experience.

6 Conclusion

The GDPR places demands on service providers to secure that users can have control of private data and that there is transparency to what happens with their data. Existing ways to put focus on privacy such as notifications and consent forms can play a higher role with the GDPR in force.

This paper, has had the purpose to understand where participants/users would find it necessary for the service provider to provide a notification or consent form in the exchange of information behind the services as a privacy reflection with the GDPR as background. Three applications have been discussed by 15 participants: The Endomondo applications, MobilePay and

Roskilde Festival application. Mental models have been created to reflect how the participants perceive how the services work for particular tasks and these models have been used to identify privacy challenges. The paper concludes that the mental models could be used to discuss privacy challenges and as basis for suggesting notifications and consent forms relating to the three applications.

References

[1] Beaumont, R. (2016). The GDPR, Cookie Consent and Customer Centric Privacy. Retrieved from: https://www.cookielaw.org/blog/2016/5/13/the-gdpr,-cookie-consent-and-customer-centric-privacy/

[2] Bjerreby, D. (2016). Click to Agree with What? No One Reads Terms of Service, Studies Confirm. Retrieved from: https://www.theguardian.com/technology/2017/mar/03/terms-of-service-online-contracts-fine-print

[3] Cavoukian, A., and Chibba, M. (2018). Start with Privacy by Design in All Big Data Applications. In *Guide to Big Data Applications*, (pp. 29–48). Springer, Cham.

[4] Centre for Information Policy Leadership (2017). Recommendations for Implementing Transparency, Consent and Legitimate Interest under the GDPR. Centre for Information Policy Leadership GDPR Implementation Project 19 May 2017.

[5] Clarke, R. (2000). Beyond OECD Guidelines: Privacy Protection for the 21st Century. Xamax Consultancy Pty Ltd. Retrieved from: http//www.rogerclarke.com/DV/PP21C.html

[6] Cranor, L. F., Guduru, P., and Arjula, M. (2005). User Interfaces for Privacy Agents. Retrieved from: lorrie.cranor.org/pubs/privacy-bird-20050714.pdf

[7] EC (2016). Protection of Personal Data. Retrieved from: http://ec.europa.eu/justice/data-protection/

[8] EU (2016a). General Data Protection Regulation, GDPR. Retrieved from: gdpr-info.eu/art-4-gdpr

[9] IBM (2015). Cloud Data Rocks Out the Roskilde Festival. Retrieved from: http://www.ibmbigdatahub.com/infographic/cloud-data-rocks-out-roskilde-festival

[10] Kang, T., Dabbish, L., Fruchter, N., and Kiesler, S. (2015). "My Data Just Goes Everywhere: User Mental Models of the Internet and Implications for Privacy and Security." *Symposium on Usable Privacy and Security (SOUPS)*, July 22–24, Ottawa, Canada.

[11] Kelley, P. G., Bresee, J., Cranor, L. F., and Reeder, R. W. (2009). A nutrition label for privacy. In *Proceedings of the 5th Symposium on Usable Privacy and Security* (p. 4). ACM.

[12] Khajuria, S., and Sørensen, L. (2015). Where Does My Private Data Go? Visualization of Users' Privacy. *48th Annual Hawaii International Conference on System Sciences*, Kauai, Hawaii, 5–8.

[13] Lamm, J. (2016). Study Shows Users Don't Read Terms of Service Agreements. Retrieved from http://www.digitalpassing.com/2016/07/14/study-shows-users-read-terms-service-agreements/

[14] Lindow-Zeichmeister, S. (2017). Privacy Management (In German). Retrieved from: https://www.android-user.de/gotchya-privacy-management-die-berechtigungen-deiner-installierten-apps-immer-im-blick/

[15] Lipert, T. (2015). Exposing the Hidden Web: An Analysis of Third-Party HTTP Requests on 1 Million Websites. *International Journal of Communication*, 9, pp. 3544–3561.

[16] Nielsen, J. (2010). Mental Models. Retrieved from: https://www.nngroup.com/articles/mental-models/

[17] NN Group (2014). Turn User Goals into Task Scenarios for Usability Testing. Retrieved from: https://www.nngroup.com/articles/task-scenarios-usability-testing/

[18] Olesen, L. (2017). Top Android and iOS-apps in Denmark (In Danish). Retrieved from: https://www.mobilsiden.dk/nyheder/top-10-android-og-ios-apps-i-danmark-marts-2017,lid.37935/

[19] Pettersson, J. S. (2012). A Brief Evaluation of Icons Suggested for Use in Standardised Information Policies – Referring to the Annex in the first reading of the European Parliament on COM (2012) 0011. Working Paper, April 2014. Karsldad Univerity, Faculty of Arts and Social Sciences.

[20] Rainie, L., and Duggan, M. (2016). Privacy and Information Sharing. Pew Research Center, December 2015, Available at: http: www.pewinternet.org/2016/01/2016/Privacy-and-Information-Sharing

[21] Shaub, F., Balebako, R., Durity, A. L., and Canor, L. F. (2015). A Design Space for Effective Privacy Notices. *Symposium on Usable Privacy and Security (SOUPS)*, July 22–24, Ottawa, Canada.

[22] Statistica (2017). retrieved from: https://www.statista.com/topics/1002/mobile-app-usage/

[23] Titcomb, J. (2016). Cookie Warnings Could Be Removed From Websites Under EU Plans. Retrieved from: http://www.telegraph.co.uk/technology/2016/12/13/cookie-warnings-could-removed-websites-eu-proposals/

[24] ToS, DR (2012). Terms of Service Didn't Read. Retrived from: https://tosdr.org/index.html
[25] Vallina-Rodriguez, N., and Sundaresan, S. (2017). 7 in 10 smartphone apps share your date with third-party services. Retrieved from: https://the conversation.com/7-in-10-smartphone-apps-share-your-data-with-third-party-services-72404
[26] Ziegeldorf, J. H., Morchon, O. C., and Wehrle, K. (2014). Privacy in the Internet of Things: Threats and Challenges. *Security and Communication Networks*, 7(12), 2728–2742.

Biography

L. Sørensen is associate professor at CMI (Center for Communication, Media and Information Technologies), Electronic Systems, at Aalborg University Copenhagen. She holds a Ph.D. in Engineering from DTU (Technical University of Denmark) and has specialized in Interaction Design, and software engineering and usable privacy. Sørensen has been a member of IEEE for many years. Furthermore, within the last 10 years, she has worked closely with the Wireless World Research Forum on for example requirement analyses of new technologies. Sørensen has published more than 100 scientific papers, reports and books.